F2

METHOD AND DEVICE FOR REMOTE IDENTITY VERIFICATION USING PERSONAL DISCRIMINATION DEVICE

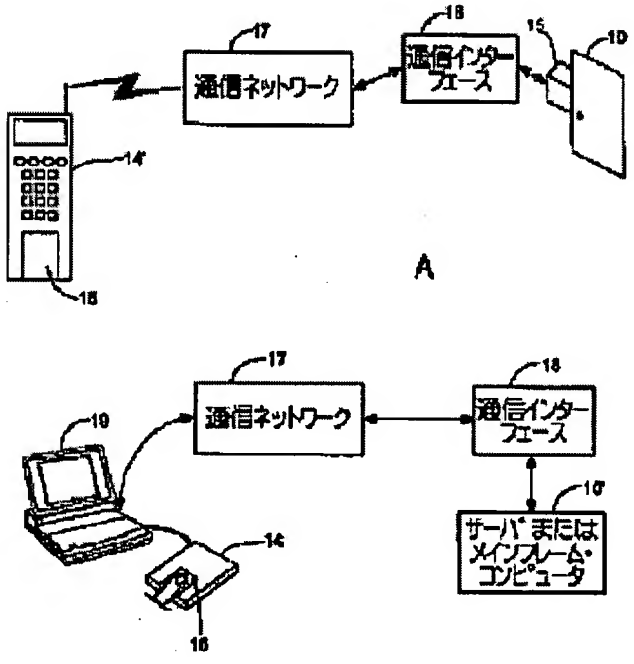
Publication number: JP11316818
Publication date: 1999-11-16
Inventor: HSU SHI-PING; LING JAMES M; MESSENGER ARTHUR F; EVANS BRUCE W
Applicant: TRW INC
Classification:
- international: ***G06K19/10; E05B49/00; G06F21/20; G06K17/00; G06Q10/00; G06Q40/00; G06Q50/00; G06T7/00; G07C9/00; H04L9/10;*** **G06K19/10; E05B49/00; G06F21/20; G06K17/00; G06Q10/00; G06Q40/00; G06Q50/00; G06T7/00; G07C9/00; H04L9/10;** (IPC1-7): G06K19/10; E05B49/00; G06F15/00; G06F19/00; G06K17/00; G06T7/00
- European: G07C9/00B6D4; G07C9/00B10; G07C9/00E6
Application number: JP19980365680 19981222
Priority number(s): US19970995565 19971222

Also published as:
EP0924657 (A2)
US6182221 (B1)
US6038666 (A1)
EP0924657 (A3)

Report a data error here

Abstract of **JP11316818**

PROBLEM TO BE SOLVED: To realize a device, which automatically verifies the identity of a person which tries to access a protection object property placed in a remote place, and a method for using this device. SOLUTION: A portable device 14' is used in a alarm system of a remote computer file or building and includes a sensor 16 which reads data like fingerprint and a collation part which compares detected data with a previously stored reference picture to discriminate it. In the case of coincidence, the device starts exchange of signals through a door 10 protecting the property and a communication network and generates a numerical value like a cyclic redundant code from the stored reference picture and enciphers this numerical value and transmits it to the door as confirmation of the identity of the person. In order to improve the safety, the person registers this numerical value for each door which he or she wants to access. When receiving confirmation of the identity from the device, the door compares the received numerical value with the numerical value stored by registration before permitting the access to the protection object property.



F2

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－316818

(43)公開日　平成11年(1999)11月16日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　19/10		Ｃ０６Ｋ　19/00	Ｓ
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｒ
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ
19/00		Ｇ０６Ｋ　17/00	Ｖ
Ｇ０６Ｔ　7/00		Ｃ０６Ｆ　15/30	３４０

審査請求　有　請求項の数20　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平10－365680

(22)出願日　平成10年(1998)12月22日

(31)優先権主張番号　９９５５６５

(32)優先日　1997年12月22日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591169755
ティーアールダブリュー・インコーポレーテッド
ＴＲＷ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国オハイオ州44124，リンドハースト，リッチモンド・ロード　1900

(72)発明者　シーピン・スー
アメリカ合衆国カリフォルニア州91107，パサディナ，サウス・ボニータ・アベニュー　461

(74)代理人　弁理士　社本　一夫　（外５名）

最終頁に続く

(54)【発明の名称】　個人識別機器を用いる遠隔同一性検証方法及び装置

(57)【要約】　（修正有）

【課題】　遠方に位置する保護対象所有物に対してアクセスしようとする人の同一性を自動的に検証する装置、およびその使用方法を提供する。

【解決手段】　遠方のコンピュータ・ファイル又は建物の警報システムを対象とする携帯機器１４’であって、指紋のようなデータを読み取るセンサ１６と、検知したデータを予め格納してある基準画像と比較、判定する照合部とを含む。一致があった場合、機器は所有物を保護するドア１０と通信ネットワークを通じて信号の交換を開始し、格納してある基準画像から巡回冗長符号のような数値を発生し、この数値を暗号化し、それを人の同一性の確認としてドアに送信する。安全性を高めるために、人はアクセスを望むドア毎にこの数値を登録する。機器からの同一性確認を受信した場合、ドアは、保護対象所有物に対するアクセスを付与する前に、受信した数値を登録の間に格納した数値と比較する。

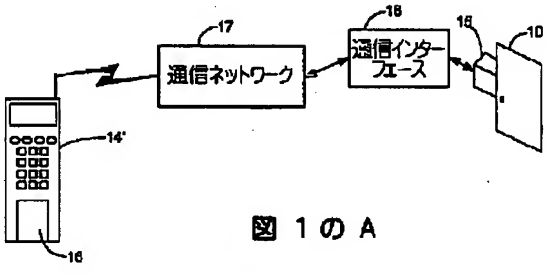


図１のＡ

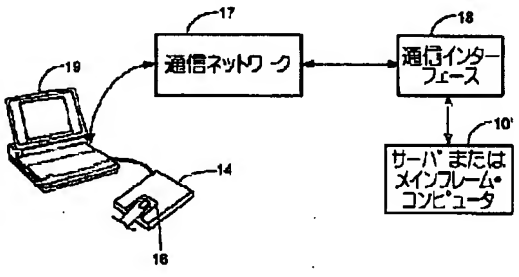


図１のＢ

【特許請求の範囲】

【請求項１】　保護対象所有物に対して遠方からアクセスを求める人の同一性を自動的に検証する装置であって、

保護対象所有物に対してアクセスを求める人を識別する生物測定学的データを読み取るセンサと、前記保護対象所有物に対してアクセスする許可を得た人を識別する基準生物測定学的データを格納する記憶手段と、前記格納してある基準生物測定学的データを、前記アクセスを求める人の生物測定学的データと比較し、これらが一致するか否かについて判定を行う照合部とを有する個人識別機器と、

通信ネットワークを通じて同一性確認を安全にドアに通信し、該ドアが、前記同一性確認の受信時に、前記保護対象所有物に対するアクセスを与えるようにする手段と、を備えた装置。

【請求項２】　請求項１記載の装置であって、更に、

検証モードにおいて前記装置の動作を開始する第１のスイッチと、前記装置を登録動作モードに置くように作動する第２のスイッチとを有するユーザ・インターフェースを備え、前記センサからの生物測定学的データを前記記憶手段に格納し、前記検証動作モードにおいて後に検索する、装置。

【請求項３】　請求項１記載の装置において、

前記センサ、前記記憶手段および前記照合部が全て、携帯通信機器に内蔵されている、装置。

【請求項４】　請求項１記載の装置において、

前記センサ、前記記憶手段および前記照合部が全て、通信機器に接続可能な携帯機器に内蔵されている、装置。

【請求項５】　請求項１記載の装置において、

前記保護対象所有物が、前記個人識別機器に対して遠方に位置するコンピュータ内に格納されているコンピュータ・ファイルである、装置。

【請求項６】　請求項２記載の装置において、前記安全に同一性確認を通信する手段が、

前記格納されている基準生物測定学的データから数値を発生する手段と、

前記数値を暗号化する暗号化ロジックと、

前記暗号化数値を、前記人に対する識別データと共に前記ドアに送る通信インターフェースと、を含み、前記送信された数値が、登録手続の間に前記人によって予め与えられたものと同じであることを確認した場合、前記ドアが前記保護対象所有物に対する所望のアクセスを与える、装置。

【請求項７】　請求項６記載の装置であって、更に、

前記ドアによって発生されかつ送信された暗号キーを受信する受信機と、

前記個人識別機器内に秘密暗号キーを格納する手段と、を備え、前記暗号化ロジックが、前記ドアから受信した前記暗号キーと前記秘密暗号キーとを用いて、前記数値に二重暗号化を施すことを特徴とする装置。

【請求項８】　遠方に位置する保護対象所有物に対するアクセスのために当該機器を用いようとするユーザの同一性を自動的に検証する個人識別機器であって、

保護対象所有物に対してアクセスしようとするユーザを識別する指紋データを読み取るセンサと、

登録手続の間に前記ユーザの基準指紋画像を格納し、今後の使用のために該基準画像を保持するメモリと、

前記格納されている基準画像を、前記アクセスしようとするユーザの前記センサから得られた指紋画像と比較し、２つの画像が一致するか否かについて判定を行う画像照合部と、

通信ネットワークを通じて同一性確認をドアに安全に通信し、該ドアが、前記同一性確認の受信時に、前記保護対象所有物に対するアクセスを与えるようにする手段と、を備えた個人識別機器。

【請求項９】　請求項８記載の個人識別機器において、

前記同一性確認を安全に通信する手段が、

前記格納されている基準指紋画像から数値を発生する手段と、

前記数値を暗号化する暗号化ロジックと、

前記暗号化数値を、前記ユーザ識別データと共に前記ドアに送る送信機と、を含み、

前記送信された数値が、登録手続の間に前記ユーザによって予め与えられたものと同じであることを確認した場合、前記ドアが前記保護対象所有物に対する所望のアクセスを与える、個人識別機器。

【請求項１０】　請求項９記載の個人識別機器において、

前記数値を発生する手段が、前記格納されている基準指紋画像から巡回冗長符号を発生する手段を含む、個人識別機器。

【請求項１１】　請求項９記載の個人識別機器であって、更に、

前記ドアによって発生されかつ送信された暗号キーを前記通信ネットワークを通じて受信する受信機と、

前記機器内に秘密暗号キーを格納する手段と、を備え、更に、

前記暗号化ロジックが、前記ドアから受信した前記暗号キーと、前記秘密暗号キーとを用いて、前記数値に二重暗号化を施す手段を含む、個人識別機器。

【請求項１２】　遠方に位置する保護対象コンピュータに対してアクセスしようとするユーザの同一性を自動的に検証する方法であって、

前記ユーザが携行する個人識別機器の一部であるセンサによって、ユーザの生物測定学的データを検知するステップと、

前記検知した生物測定学的データを、前記個人識別機器内に予め格納してある基準生物測定学的データと比較するステップと、

前記検出した生物測定学的データが前記基準生物測定学的データと一致するか否かについて判定を行うステップと、
一致があった場合、前記保護対象コンピュータに対するアクセスを制御するドアに、通信ネットワークを通じて同一性確認を安全に通信するステップと、
前記ドアにおいて前記ユーザの同一性を確認した場合、前記保護対象コンピュータに対して所望のアクセスを与えるステップと、を含む方法。
【請求項１３】　請求項１２記載の方法であって、更に、
手動スイッチによって、前記個人識別機器の検証動作を開始するステップを含む、方法。
【請求項１４】　請求項１２記載の方法において、前記安全に通信するステップが、
前記格納されている基準生物測定学的データから数値を発生するステップと、
前記数値を暗号化するステップと、
前記通信ネットワークを通じて前記暗号化数値を前記ドアに送信するステップと、
前記通信ネットワークを通じてユーザ識別データを前記ドアに送信するステップと、
前記ドアにおいて、前記暗号化数値を受信しかつ解読するステップと、
前記ドアにおいて登録プロセスの間に前記ユーザによって予め格納されている数値と、前記解読した数値とを比較し、前記ユーザの同一性を確認するステップと、
前記ユーザの同一性が確認された場合、所望の機能を活性化させ、前記保護対象コンピュータに対するアクセスを与えるステップと、を含む方法。
【請求項１５】　請求項１４記載の方法において、前記安全に通信するステップが、更に、
前記ドアにおいて、ドア公開暗号キーおよびドア秘密暗号キーのランダム対を発生するステップと、
前記ドア公開キーを前記個人識別機器に送信するステップと、
前記機器のそれ以降のあらゆる使用のために、公開および秘密暗号キーの対を、前記個人識別機器に対して選択するステップと、
前記ドア登録プロセスの一部として、前記個人識別機器の公開キーを前記ドアに与えるステップと、
前記個人識別機器の秘密キーを前記機器内に機密的に格納するステップと、を含み、
前記暗号化ステップが、前記ドアの公開キーおよび前記個人識別機器の秘密キーを用いて、前記数値に二重暗号化を施すステップを含む、方法。
【請求項１６】　請求項１５記載の方法において、前記ドアが、
前記個人識別機器の公開キーおよび前記ドアの秘密キーを用いて、前記二重に暗号化された数値を解読する追加のステップを実行する、方法。
【請求項１７】　遠方に位置する保護対象コンピュータに対するアクセスをユーザが得るための方法であって、
ドアに近づきつつ、機器内の指紋センサ上に指を置くステップと、
前記機器を作動させ、前記ユーザの指紋を検知しかつ記録するステップと、
前記検知した指紋を、前記機器内に予め格納してある基準指紋データと比較するステップと、
比較において合格した場合、前記機器から、前記保護対象コンピュータに通信ネットワークを通じて同一性確認を送信するステップと、
同一性確認の受信時に、前記保護対象コンピュータに対して要求されたアクセスを与えるステップと、を含む方法。
【請求項１８】　請求項１７記載の方法において、前記同一性確認を送信する前記ステップが、
前記機器において前記同一性確認を暗号化するステップと、
前記保護対象コンピュータにおいて前記同一性確認を解読するステップと、を含む方法。
【請求項１９】　請求項１８記載の方法において、
前記暗号化ステップが、二重暗号化を施すステップを含み、
前記解読ステップが、二重に解読するステップを含む、方法。
【請求項２０】　請求項１９記載の方法において、
前記二重暗号化を施すステップが、最初に、前記保護対象コンピュータ内において発生し、そこから受信した公開ドア暗号キーを用いて、前記同一性確認を暗号化し、次いで前記機器内に格納されている秘密機器暗号キーを用いて更に暗号化を行うステップを含み、
前記二重に解読するステップが、最初に、前記コンピュータにおける以前の登録時に前記ユーザによって与えられた公開機器暗号キーを用いて解読を行い、次いで前記コンピュータにおいて発生した秘密暗号キーを用いて解読を行うステップを含む、方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、一般的に、個人識別または検証システムに関し、更に特定すれば、貴重な情報に対するアクセスを許可する前、または種々のトランザクションを遠方から実行する機能を付与する前に、人の同一性（ｉｄｅｎｔｉｔｙ）を自動的に検証するシステムに関するものである。
【０００２】
【従来の技術】従来より、所有物（ｐｒｏｐｅｒｔｙ）にアクセスする権利を有する人のみが必要な鍵またはダイヤル錠用コンビネーション（ｃｏｍｂｉｎａｔｉｏｎ）を有するという理論に基づいて、鍵および錠、また

は組み合わせ錠（ダイヤル錠）を用いて、当該所有物に対するアクセスを制限している。勿論、この従来からの手法は、部屋、建物、自動車および銀行内の貸し金庫（ｓａｆｅ　ｄｅｐｏｓｉｔｂｏｘ）を含む種々の閉鎖空間に対するアクセスを制限するために、今でも広く用いられている。近年、機械的な錠は、例えば、ホテルの部屋のドア、または銀行の自動預金支払機（ＡＴＭ：ａｕｔｏｍａｔｉｃ　ｔｅｌｌｅｒ　ｍａｃｈｉｎｅ）に対するアクセスに用いられるような、符号化プラスチック・カードによって作動する電子的な錠に取って代わられつつある。後者の場合、銀行口座の「キー」のようなプラスチック・カードのユーザは、アクセスが許可されるには、同様に個人識別番号（ＰＩＮ）を入力しなければならない。

【０００３】電話によって、またはその他の何らかの形式の通信ネットワークを通じて、ある人が遠方から情報にアクセスしようとする場合、全く異なる問題が生じる。電話による同一性の検証は、典型的に、パスワード、個人識別番号（ＰＩＮ）、または限られた数の人だけが知っている単語を用いて行われる。銀行では、顧客の母親の旧姓をアクセス・コードとして用いる場合が多く、時として、理論的に顧客のみにわかっている他のコードまたは番号と結合させている。この手法には多くの実用上の問題があり、その内最も明白なのは、これらのコードまたは秘密の単語が、盗まれたり、消失したり、あるいはその他の手段によって悪用される危険性があることである。同一性データをプラスチック製識別カード上の磁気ストライプに符号化し、これを適切なカード読取装置を有する電話機と共に用いることによって、安全性を向上させることができる。集積回路チップ上に更に多くの情報を収容する「スマート・カード」の使用も提案されているが、これらの手法にも、同一性カードを紛失したり、盗まれたりする場合があるという欠点がある。

【０００４】

【発明が解決しようとする課題】したがって、情報および資産に対して安全なアクセスを与える、信頼性を高めた技術に対する必要性が、特に、ある種の通信システムを通じてこのアクセスを得ようとするユーザにとって、広く存在している。理想的には、この技法は、遠方からのアクセスを得ようとするする人の同一性を確実に検証し、多数のスキャナブル・カード（ｓｃａｎｎａｂｌｅ　ｃａｒｄ）を携行する必要性や、コンビネーション、パスワードおよびＰＩＮを記憶する必要性をなくすべきである。本発明は、この要望を満たすものである。

【０００５】

【課題を解決するための手段】本発明は、保護対象所有物に遠方よりアクセスしようとする人の同一性を自動的に検証する装置およびその使用のための方法にある。保護対象所有物は種々の形態を取り得るが、典型的に、ユーザが情報を読み出したりあるいは書き込んだりするためにアクセスしようとする、遠方に位置するコンピュータを含む。あるいは、保護対象所有物は、建物またはその他の構造物であり、ユーザは、かかる建物において警報システムの活性化および不活性化を行うことを望む場合もある。

【０００６】端的にそして一般的なことばで述べると、本発明の装置は、個人識別機器と、同一性確認をドアに安全に通信し、ドアが同一性確認の受信時に保護対象所有物に対するアクセスを与えるようにする手段とを備えている。個人識別機器は、保護対象所有物に対してアクセスしようとする人を識別する生物測定学的（ｂｉｏｍｅｔｒｉｃ）データを読み取るセンサと、保護対象所有物に対してアクセスする許可を得た人を識別する基準生物測定学的データを格納する記憶手段と、格納してある基準生物測定学的データを、アクセスしようとする人の生物測定学的データと比較し、これらが一致するか否かについて判定を行う照合部（相関器）とを含む。本装置は、更に、検証モードにおいて本装置の動作を起動する第１のスイッチと、本装置を登録動作モードに置くように作動する第２のスイッチとを有するユーザ・インターフェースを備え、センサからの生物測定学的データを記憶手段に格納し、検証動作モードにおいて後に検索する。

【０００７】開示する本発明の実施形態の１つでは、センサ、記憶手段および照合部は全て、電話機のような携帯通信機器、または保護対象所有物から離れた、他の何らかの形式の通信機器に内蔵されている。携帯通信機器としては、人が携行する機器とすればよい。開示する実施形態では、安全に同一性確認を通信する手段は、格納されている基準生物測定学的データから数値を発生する手段と、数値を暗号化する暗号化ロジックと、暗号化数値を、人に対する識別データと共にドアに送る通信インターフェースとを含む。送信された数値が、登録手続の間に人によって予め与えられたものと同じであることを確認した場合、ドアが保護対象所有物に対する所望のアクセスを与える。

【０００８】本発明の装置は、更に、ドアによって発生されかつ送信された暗号キーを受信する受信機と、識別機器内に秘密暗号キーを格納する手段とを備えることも可能である。更に、機器内の暗号化ロジックは、ドアから受信した暗号キーと秘密暗号キーとを用いて数値に二重暗号化を施す。

【０００９】また、本発明の装置は、別個の機器として規定することも可能であり、この機器は、保護対象所有物に対してアクセスしようとするユーザを識別する指紋データを読み取るセンサと、登録手続の間にユーザの基準指紋画像を格納し、今後の使用のために該基準画像を保持するメモリと、格納されている基準画像を、アクセスしようとするユーザのセンサから得られた指紋画像と

比較し、２つの画像が一致するか否かについて判定を行う画像照合部と、同一性確認をドアに安全に伝達し、ドアが、同一性確認の受信時に、保護対象所有物に対するアクセスを与えるようにする手段とを含む。更に具体的には、同一性確認を安全に伝達する手段は、格納されている基準指紋画像から数値を発生する手段と、数値を暗号化する暗号化ロジックと、暗号化数値を、ユーザ識別データと共にドアに送る送信機とを含む。送信された数値が、登録手続の間にユーザによって予め与えられたものと同じであることを確認した場合、ドアが保護対象所有物に対する所望のアクセスを与える。

【００１０】直前の段落において規定したような個人識別機器では、数値を発生する手段は、格納されている基準指紋画像から巡回冗長符号を発生する手段を含む。この機器は、更に、ドアによって発生されかつ送信された暗号キーを受信する受信機と、機器内に秘密暗号キーを格納する手段とを含む。この機器内の暗号化ロジックは、ドアから受信した暗号キーと、秘密暗号キーとを用いて、数値に二重暗号化を施す手段を含む。

【００１１】遠方に位置する保護対象コンピュータに対してアクセスしようとするユーザの同一性を自動的に検証する新規の方法に関して、本発明は、ユーザが携行する個人識別機器の一部であるセンサによって、ユーザの生物測定学的データを検知するステップと、検知した生物測定学的データを、個人識別機器内に予め格納してある基準生物測定学的データと比較するステップと、検出した生物測定学的データが基準生物測定学的データと一致するか否かについて判定を行うステップと、一致があった場合、保護対象所有物に対するアクセスを制御するドアに、通信ネットワークを通じて同一性確認を安全に伝達するステップと、ドアにおいてユーザの同一性を確認した場合、保護対象コンピュータに対して所望のアクセスを与えるステップとから成る。本方法は、更に、手動スイッチによって、個人識別機器の通常動作を開始するステップを含む。

【００１２】本方法の一実施形態では、安全に通信するステップは、格納されている基準生物測定学的データから数値を発生するステップと、数値を暗号化するステップと、暗号化数値をドアに送信するステップと、ユーザ識別データをドアに送信するステップと、ドアにおいて、暗号化数値を受信しかつ解読するステップと、ドアにおいて登録プロセスの間にユーザによって予め格納されている数値と、解読した数値とを比較し、ユーザの同一性を確認するステップと、ユーザの同一性が確認された場合、所望の機能を活性化させ、保護対象コンピュータに対するアクセスを与えるステップとを含む。

【００１３】更に具体的には、安全に伝達するステップは、更に、ドアにおいて、ドア公開暗号キーおよびドア秘密暗号キーのランダム対を発生するステップと、ドア公開キーを個人識別機器に送信するステップと、機器のそれ以降のあらゆる使用のために、公開および秘密暗号キーの対を、個人識別機器に選択するステップと、ドア登録プロセスの一部として、個人識別機器の公開キーをドアに与えるステップと、個人識別機器の秘密キーを機器内に機密的に格納するステップとを含む。暗号化ステップは、ドアの公開キーおよび個人識別機器の秘密キーを用いて、数値に二重暗号化を施すステップを含む。本方法は、更に、個人識別機器の公開キーおよびドアの秘密キーを用いて、二重に暗号化された数値を解読する追加のステップを実行するステップを含み、このステップはドアにおいて実行される。

【００１４】また、本発明は、遠方に位置する保護対象コンピュータに対するアクセスをユーザが得るための方法として規定することも可能であり、この方法は、機器内の指紋センサ上に指を置くステップと、機器を作動させ、ユーザの指紋を検知しかつ記録するステップと、検知した指紋を、機器内に予め格納してある基準指紋データと比較するステップと、比較において合格した場合、機器から保護対象コンピュータに通信ネットワークを通じて同一性確認を送信するステップと、同一性確認の受信時に、保護対象コンピュータに対して要求されたアクセスを与えるステップとを含む。理想的には、同一性確認を送信するステップが、機器において同一性確認を暗号化するステップと、保護対象コンピュータにおいて同一性確認を解読するステップとを含む。更に具体的には、機器における暗号化は、保護対象コンピュータから受信した公開暗号キーおよび機器に格納してある秘密暗号キーを用いて二重に暗号化することを含み、解読は、機器のユーザが与える公開キーおよびコンピュータ内で発生する秘密暗号キーを用いて二重に解読することを含む。

【００１５】以上の説明から、本発明は、遠方に位置するコンピュータまたは同様の保護対象所有物に対して安全なアクセスを与えるという点において、飛躍的な進歩を意味することが認められよう。即ち、本発明は、セキュリティ機器を用いて多数の所有物または資産に遠方よりアクセスすることを可能にする。この防犯機器は、指紋のような生物測定学的なデータを用いて、その所有者を信頼性高く識別する。識別は小型の携帯機器内で検証されるので、保護対象所有物への多数の「ドア」との通信は単純な同一性確認メッセージに限定し、これに適切な暗号化を施すことによって、盗聴またはリバース・エンジニアリングを防止することができる。本発明のその他の態様および利点は、添付図面と関連付けた、以下の更に詳細な説明から明らかとなろう。

【００１６】

【発明の実施の形態】例示の目的で図面に示すように、本発明は、通信ネットワークを通じて保護対象所有物に遠方からアクセスしようとする人の同一性を自動的に検証するシステムに関するものである。従来、保護対象所

有物に対する遠方からのアクセスは、パスワード、コードおよび同様の機構を用いることによって制御してきた。

【００１７】本発明によれば、保護対象所有物にアクセスしようとする人は、その人に関連する、選択した生物測定学的測定値を得ることができるセンサを含む携帯識別機器を携行し、保護対象所有物の「ドア」付近に位置する関連機器と通信する。好ましくは、携帯機器は同一性検証手段も含み、センサから得た生物測定学的測定値を、予め行われた登録手続の間に同じ人から得た１組の基準生物学的測定値に含まれる、対応する測定値と比較する。

【００１８】図１Ａは、保護対象所有物への「ドア」を開くために本発明をいかにして用いるかを概略的に示す。ドアを参照番号１０で示す。ドア１０に入ろうとする人は、小型ハンドヘルド機器を携行する。このハンドヘルド機器は、セルラ電話機１４’に一体化することができ、あるいは別個の機器（図１Ｂ）の形態を取ることも可能である。しかしながら、ハンドヘルド機器がその他の種類の通信端末に一体化される場合もあることは理解されよう。電話機１４’は、ドア１０付近に配置された受信機１５と通信する。本発明のこの好適な実施形態では、電話機１４’は生物測定学的センサを含み、この好適な実施形態ではそれは指紋センサ１６である。しかしながら、本発明の原理は、解剖学的構造の他の部分からの印刷パターン、または目の虹彩パターンのように、ユーザを識別する他の生物測定学的特性を採用する装置にも適用可能であることは理解されよう。

【００１９】電話機１４’は、通信ネットワーク１７およびドア１０付近に位置する通信インターフェース１８を通じて、受信機１５と通信する。インタフェース１８は、例えば電話機とすることができる。図１のＢは、いかにして指紋センサ１６をラップトップ・コンピュータ１９に接続し得るかを示す。遠方に位置するコンピュータは、他の形態の「ドア」を具体化するものであるので、１０’で示すことにする。ユーザが、コンピュータ１０’内の情報にアクセスしたい場合、ユーザはセンサ１６をラップトップ・コンピュータ１９に接続し、通信ネットワーク１７および通信インターフェース１８を通じてコンピュータ１０’に対する接続を行い、次いでセンサによって識別される。

【００２０】ユーザがセンサ１６上に指を置き、スイッチを作動させると、ユーザの指紋が走査され、機器１４または１４’内に格納してある基準指紋画像と比較される。機器１４または１４’は、この目的のために、指紋照合部（図１Ａおよび１Ｂには図示せず）を含む。比較の結果、一致が得られた場合、機器１４／１４’は確認メッセージをドア１０またはコンピュータ１０’に送信する。ドア１０は開いてユーザ１２によるアクセスが許可される。あるいは、コンピュータ１０’を調整して、ユーザによるデータ・アクセスを許可する。

【００２１】ドア１０またはコンピュータ１０’に送られる確認メッセージの性質は非常に重要である。何故なら、標準的なフォーマットの単純な「ＯＫ」または「開放」信号では、「クローン（ｃｌｏｎｉｎｇ）」プロセスにおいて容易に複製が作られ、無許可のアクセスは比較的単純に行われてしまうからである。理想的には、確認メッセージは、異なるアクセス「ドア」に対して同じフォーマットであるが、その複製を防止し、かつ機器１４のリバース・エンジニアリングを防止するような方法で符号化または暗号化したものでなければならない。これらの目標を達成するための一技術の詳細について、以下で説明する。

【００２２】図2は、機器１４の主要構成部品を示し、その中には指紋センサ１６、プロセッサ・モジュール２０、トランシーバ（送受信機）２２およびバッテリ電源２４が含まれる。セルラ電話機１４’のような他の機器に、同じ構成部品を一体化してもよく、更にバッテリ電源２４を電話機のバッテリと一体化してもよいことは理解されよう。指紋センサ１６は、入手可能な設計のものであればいずれでもよく、容量式センサ、光学式センサまたはその他のセンサを含むことができる。センサ１６は、ユーザの指紋の一部分の２進またはグレースケール・イメージ（画像）を生成する。迅速な処理のためには、続く比較プロセスでは、画像全体を用いない方がよく、代わりにセンサ１６が供給するのは、指紋の嶺および谷の全てを含む、指紋の詳細な「マップ」である。プロセッサ・モジュール２０を、図３に詳細に示す。

【００２３】プロセッサ・モジュール２０は、プロセッサ２６を含み、これは、例えば、ＲＩＳＣ（縮小命令セット・コンピュータ）プロセッサ、本発明の好適な実施形態における特徴照合部（ｃｏｒｒｅｌａｔｏｒ）２８である指紋一致検出部、巡回冗長符号（ＣＲＣ）発生部３０、基準指紋画像用記憶部３２、暗号化ロジック３４および秘密（プライベート）暗号キー用記憶部３６を含むことができる。また、機器１４は、ユーザ・インターフェース３８も含み、ユーザ１２はこれを通じて種々のモードの動作を起動する。基本的に、ユーザ・インターフェース３８は、指紋センサ１６に組み込んでもよい１つの主動作ボタンと、登録モードにおける動作を起動する少なくとも１つの追加ボタンとを含む。プロセッサ２６の主要な機能は、センサ１６が供給する指紋画像を前処理し、強調することである。前処理は、画像の「明瞭化」、背景効果を排除するための画像のクロッピング（ｃｒｏｐｐｉｎｇ）、画像のコントラストの強調、処理容易性が高い２進形態への画像変換を含む。登録モードでは、前処理された画像は、破線４０で示すように、基準画像記憶エリア３２内に格納される。登録は、ユーザが最初に機器１４を入手したときに行われ、通常機器を紛失するか損傷しない限り繰り返さない。防犯性およ

び利便性を高めるために、２つの指紋を登録するようにユーザに問い合わせ、例えば、ユーザが指をけがした場合でも引き続きアクセスできるようにすることが可能である。検証動作モードでは、線４３で示すように、前処理された指紋画像を照合部（相関器）２８に入力し、線４４を通じて記憶部３２から得た基準画像と比較する。照合部２８は、適切な技法を用いて、所望の防犯レベルに応じて画像を比較する。処理速度は重要な要素であるので、画像全体のビット毎の比較は通常行わない。代わりに、基準画像の重要な特徴を識別し、新たに走査した画像において同じ特徴を探す。機器１４の用途によっては、米国特許第５，０６７，１６２号に開示された技法を、例えば、照合部２８に組み込むとよい。好ましくは、指紋照合部２８は、発明者ブルースW．エバンスその他（Ｂｒｕｃｅ　Ｗ．　Ｅｖａｎｓ　ｅｔ　ａｌ．）による「指紋特徴照合装置」（Ｆｉｎｇｅｒｐｒｉｎｔ　Ｆｅａｔｕｒｅ　Ｃｏｒｒｅｌａｔｏｒ）と題する同時係属中の特許出願の教示に従うとよい。その内容は、この言及により、この明細書にも含まれるものとする。画像比較の結果として、照合部２８は、線４６上に一致信号を発生することができ、これがＣＲＣ発生部３０を活性化する。線４８上に示すように不一致信号が発生した場合、それ以上の処理は行われない。任意選択肢（オプション）として、線４８上の不一致信号を用いて、ユーザ・インターフェース３８上のインディケータを作動させてもよい。

【００２４】線４６上の一致信号によって、巡回冗長符号（ＣＲＣ）発生部３０を作動させると、基準画像データから導出した比較的長い（１２８ビットのような）二進番号を発生する。ＣＲＣは、単一の番号を与え、全ての実用的な目的のために、格納されている基準指紋画像を一義的に識別する。２つの指紋画像が同じＣＲＣを生成することは、非常に可能性は低いが、その場合でも、本発明のシステムの安全性を損なうことはない。これについては以下で明らかとなろう。

【００２５】ＣＲＣ自体は機器１４には格納されず、暗号化された形態でドア受信機１５に送信される。特定のドア１０に初めてアクセスするために機器１４を使用する前に、ユーザ１２は最初にドアに「登録」しなければならない。登録プロセスは、ドアの管理者がユーザ名（口座番号、またはその他の識別情報）を、ユーザの機器１４に用いられる公開暗号キーおよびユーザの基準指紋から得られるユーザのＣＲＣと関連付けて格納するプロセスである。例えば、ドア１０が金融機関に対するアクセスを与える場合、ユーザは、登録する際に、彼または彼女の機器１４を当該機関に持ち込み、機器から指紋ＣＲＣをドア受信機１５に送信する。登録モードでは、ドア受信機１５は、ユーザ名またはその他識別情報と関連付けて、ユーザのＣＲＣを格納する。登録プロセスの一部として、ユーザ１２には、機器１４以外に何らかの識別を提示することが通常要求され、そのユーザが実際に氏名またはその他の識別情報を提示した人であり、それがドア１０に格納される人であることを金融機関に証明する。

【００２６】以下で更に詳細に説明するが、ユーザが登録し終えたドア１０に後にアクセスするために機器１４を使用する場合、機器はユーザ名および格納されている基準画像に対応するＣＲＣを送信する。すると、ドア１０またはコンピュータ１０’のロジックが、受信したＣＲＣを、登録の間にユーザ名と共に格納したＣＲＣと比較する。一致が有れば、そのユーザのためにドアが開かれる。

【００２７】図4は、個人識別機器１４とドア１０との間で授受される通信を示し、コンピュータ１０．１、および遠方からのアクセスが望まれる家またはその他の所有物におけるような、その他の種類の「ドア」１０．２という２つの異なる形態が示されている。各ドア１０はアクチュエータ５０を有し、ドアの開放のような、何らかの所望の動作を行う。また、各ドアはデータベース５２も有し、その中にユーザ名、ユーザ機器の公開暗号キーおよびユーザのＣＲＣを、ドアを使用するために登録した各ユーザ毎に格納してある。コンピュータ１０．１に対するファイル・アクセスでは、ユーザは、銀行またはその他の機関におけるユーザ口座に関連する個人データに単にアクセスすればよく、あるいはコンピュータ内のファイルから情報をダウンロードする必要がある場合もある。ドア１０．２に対するアクセスでは、ユーザは、例えば、警報システムが住居または事務所において活性化されていることを確かめる必要がある場合もある。

【００２８】ユーザが機器１４を作動させると、線５４で示すように、ユーザ名が暗号化されない状態でドア１０に送信される。ドア１０は、ユーザ名を受信すると、続くメッセージの交換に用いるために、公開暗号キーおよび秘密暗号キーのランダム対を発生する。本発明のこの例示の実施形態では公開キー暗号方式を用いるので、多少の説明は必要であろうが、公開キー暗号方式の原理は安全な通信の分野ではよく理解されていることは認められよう。

【００２９】公開キー暗号方式では、２つの別個の暗号キー、即ち、「公開」キー（誰にでも知られ得るものであり、秘密に保持されていない）および「秘密（プライベート）」キー（一方から他方への通信において、一方にのみ知られている）を用いる。公開キー－秘密キーの対は、これらのいずれかを用いてメッセージを暗号化する場合、その対の他方によってそのメッセージを解読するという特性を有する。例えば、Ａ側が、最初にＢ側の公開キーを用いて暗号化することによって、機密メッセージをＢ側に送ることができる。Ｂのみがこのメッセージを解読することができる。何故なら、解読に必要なＢ

の秘密キーを有するのはＢだけであるからである。同様に、Ｂは、暗号化にＢの秘密キーを用いて、暗号化メッセージをＡに送ることも可能である。Ａは、Ｂの公開キーを用いてメッセージを解読することができるが、誰でもこれを行うことができる。何故なら、Ｂの公開キーは他の者にも知られているからである。したがって、この公開キー暗号方式の「逆方向」形態（ｂａｃｋｗａｒｄ　ｆｏｒｍ）を用いてメッセージを送信すると、安全ではない場合もある。

【００３０】本発明の図示の実施形態は、公開キー暗号方式の二重暗号形態を用いる。機器１４およびドア１０双方が公開キー－秘密キー対を有する。ここで考えられることは、本発明の機器１４は「固定」の公開および秘密キー対を有することである。即ち、公開および秘密キーを機器のユーザ毎に変更しないのである。機器の公開キーは各ドア１０に登録されており、その使用毎に変更することは実用的でない。機器の秘密キーは機器１４に格納され（図3の３６）、検査やリバース・エンジニアリングによって認識され得ないような形態とすることが好ましい。例えば、通常のどのリバース・エンジニアリング技法でも実際には解読不可能となるように、プロセッサ・モジュール２０のシリコン構造内にキーを符号化する。各ドア１０は、当該ドアが新たに使用される毎に、新たな公開－秘密キー対を発生する。このようにすれば、実際の機器１４とのメッセージ交換に先立って、これらのキーを判定することはできない。

【００３１】機器１４からユーザ名を受信すると、アクセスされようとしているドア１０は、公開－秘密キーのランダム対を発生し、線５８で示すように、暗号化せずにこの公開キーを機器に送信する。次に、機器１４は、検知した指紋画像と基準画像がうまく一致して、ユーザ識別の有効性を判定した場合、機器１４は、発生したＣＲＣに対して、２レベルの暗号化を行う。最初に、機器１４内の暗号化ロジック３４がドアの公開キーを用いてＣＲＣを暗号化する。次に、得られた暗号化ＣＲＣに対して、機器の秘密キーを用いて、二重暗号化を行う。二重暗号化ＣＲＣはドア１０に送信され、機器の公開キーを用い、次いでドアの秘密キーを用いて解読され、ＣＲＣを復元する。次に、ドア１０は、このＣＲＣを、ドアにアクセスしようとしているユーザの名前と関連付けられている、データベース５２内のＣＲＣと比較する。一致があれば、ドア１０はそのアクチュエータ５０にドアを開くように、またはそれ以外の何らかの所望の動作を行うように指令する。

【００３２】この説明から、本発明は保護対象所有物へのアクセスのために非常に安全な技術を提供することが認められよう。機器１４は、最初にユーザの指紋が格納されている基準画像と一致しなければ、ドア開放動作を開始することができないように設計されている。機器を盗んだ者が自身の指紋を機器内にうまく再登録したとしても、本当のユーザが登録されている各ドアに格納されているＣＲＣが、泥棒によるドアの動作を防止する。

【００３３】「クローン」機器を製作しようとしても、機器の秘密キーを有することができないので、ドアは、クローン機器からのメッセージを解読することができないであろう。ある者が機器の送信を傍受し、その後同じドアを開けようとする試みにおいて、このメッセージをエミュレートしようとした場合、ドアはトランザクション毎に異なる組のキーを用いるために、このたくらみは失敗に終わるであろう。このように、機器の暗号化メッセージは、いずれのドアに対しても、１回１回異なるものとなる。

【００３４】ドア１０にＣＲＣを最初に暗号化した形態で格納しておくことにより、更に防犯レベルを強化し、ドアからＣＲＣが盗まれるのを防止することも可能である。

【００３５】ドア１０がコンピュータ１０．１であり、ユーザがコンピュータから情報をダウンロードしたい場合、これは、機器１４とコンピュータ１０．１との間で追加のメッセージ交換を行い、コンピュータからの転送のために適切なレベルの安全性を確立することが通常必要である。この安全なデータ伝送を行うための技法には、伝送のためのセッション暗号キーを確立するためのメッセージの交換を含む場合があり、あるいは暗号キーをこの目的のために予め確立しておいてもよい。

【００３６】以上の説明から、本発明は、防犯機器の分野において、遠方の所有物に対するアクセスを制限するための格段の進歩を表すことが理解されよう。即ち、本発明は、ハンドヘルド機器を用い、指紋に見られるような、一意の生物測定学的パラメータを用いることによって、その所有者の同一性を極めて信頼性高く検証することにより、人が遠方から多くの異なる所有物に対するアクセスを得ることを可能にする。更に、本発明の装置は、リバース・エンジニアリング、「クローン技術」、および保護対象所有物に対するアクセスを得るためのその他の改竄技法に対して高い抵抗力を有する。また、本発明の具体的な実施形態は、例示の目的のために詳細に説明したが、本発明の精神および範囲から逸脱することなく種々の変更も可能であり、特許請求の範囲以外による限定は受けないものとすることは認められよう。

【図面の簡単な説明】

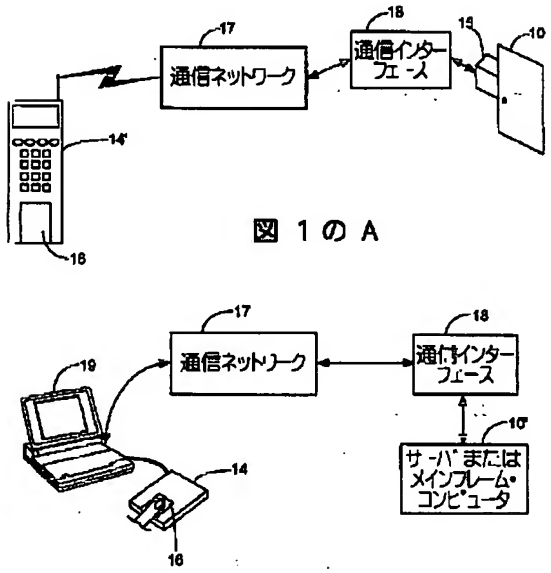
【図１】図１Ａは、セルラ電話機に一体化した個人識別機器を用いて、通信ネットワークを通じて遠方からドアを開く場合の、本発明の応用を示す図である。図１Ｂは、個人識別機器を携帯コンピュータと共に用いて、遠方に位置するコンピュータに対するアクセスを得る場合を示すブロック図である。

【図２】本発明の主要な構成部品を示すブロック図である。

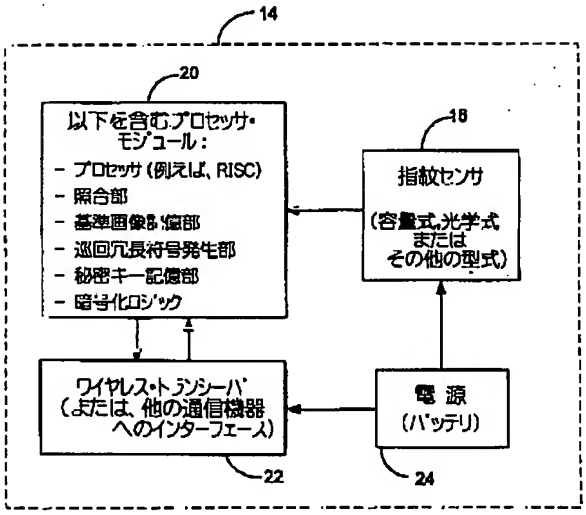
【図３】図２に示すプロセッサ・モジュールの構成部品

を示す、更に詳細なブロック図である。
【図4】携帯機器と保護対象所有物へのドアとの間で送信される一連の信号を示すブロック図である。
【符号の説明】
10　ドア
10．1　コンピュータ
10．2　ドア
12　ユーザ
14　セルラ電話機
15　受信機
16　指紋センサ
20　プロセッサ・モジュール
22　トランシーバ
24　バッテリ電源
26　プロセッサ
28　特徴照合部
30　巡回冗長符号（CRC）
32　基準指紋画像用記憶部
34　暗号化ロジック
36　秘密暗号キー用記憶部
38　ユーザ・インターフェース
50　アクチュエータ

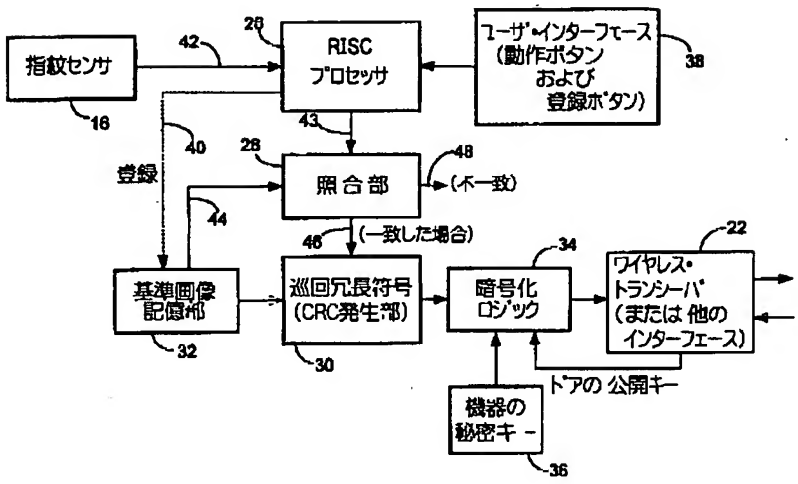
【図1】



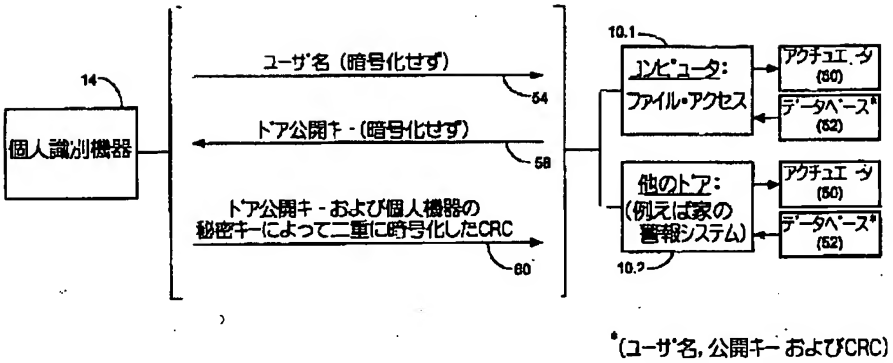
【図2】



【図3】



【図４】



フロントページの続き

(51)Int.Cl.[6]　　識別記号　　ＦＩ
ＧＯ６Ｋ　17/00　　ＧＯ６Ｆ　15/62　　４６０

(72)発明者　ジェイムズ・エム・リン
アメリカ合衆国ヴァージニア州22066，グレート・フォールズ，ジェイスミス・ストリート　929

(72)発明者　アーサー・エフ・メッセンジャー
アメリカ合衆国カリフォルニア州90278，レドンド・ビーチ，ヴァンダービルト・レーン　2618，アパートメント・ビー

(72)発明者　ブルース・ダブリュー・エヴァンス
アメリカ合衆国カリフォルニア州90277，レドンド・ビーチ，マリーナ・ウェイ　220，ナンバー　３